John J. Nelson (SBN 317598)
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

*Attorney for Plaintiff and The Proposed Class*

**UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF CALIFORNIA**

| | |
|---|---|
| **E.H.,** individually and on behalf of all others similarly situated, by her parent and guardian ELIZABETH SPENCE,<br><br>Plaintiff,<br><br>v.<br><br>POWERSCHOOL HOLDINGS, INC.<br><br>Defendant. | **Case No.:**<br><br>**COMPLAINT – CLASS ACTION**<br><br>**FOR DAMAGES, INJUNCTIVE RELIEF, AND EQUITABLE RELIEF FOR:**<br><br>**1. NEGLIGENCE**<br>**2. NEGLIGENCE *PER SE***<br>**3. BREACH OF CONTRACT**<br>**4. UNJUST ENRICHMENT**<br>**5. BREACH OF CONFIDENCE**<br><br>**JURY TRIAL DEMANDED** |

Plaintiff E.H ("Plaintiff"), by her parent and guardian Elizabeth Spence, individually and on behalf of all others similarly situated, brings this Class Action Complaint against PowerSchool Holdings, Inc. ("PowerSchool" or "Defendant"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff,

## INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted PowerSchool Holdings, Inc. with sensitive personally identifiable

information ("PII"[1]) and protected health information ("PHI" and collectively, "Private Information") that was impacted in a data breach that Defendant publicly disclosed in January 2025 (the "Data Breach" or the "Breach").

2. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information.

3. Defendant is a cloud-based software solutions provider for K-12 schools and districts that supports over 60 million students and over 18,000 customers worldwide, and is headquartered in Folsom, California.[2]

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. On December 28, 2024, Defendant became aware of a security incident on its IT Network.[3] Defendant launched an investigation to determine the nature and scope of the incident.[4]

6. The investigation determined that an unauthorized third-party gained access to Defendant's IT Network between December 22, 2024, and December 28, 2024. and obtained individuals' sensitive Private Information through PowerSchool's customer support portal, PowerSource.[5]

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] *PowerSchool Holdings, Inc*.: https://www.powerschool.com/company/ (last visited January 10, 2025).

[3] Lawrence Abrams, *PowerSchool hack exposes student, teacher data from K-12 districts* (January 7, 2025) https://www.bleepingcomputer.com/news/security/powerschool-hack-exposes-student-teacher-data-from-k-12-districts/ (last visited January 10, 2025).

[4] *Id.*

[5] *Id.*

7. PowerSchool's investigation determined that an unauthorized third-party gained access to PowerSource by using compromised credentials.[6]

8. Upon information and belief, Defendant's investigation determined that the following types of Private Information were compromised in the Data Breach: name, addresses, phone number, Social Security number, grade point average, bus stop, password, note, alert, student ID number, parent information, and medical information.[7]

9. Defendant failed to take precautions designed to keep individuals' Private Information secure.

10. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information it collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

11. Defendant admits that information in its system was accessed by unauthorized individuals, though it provided little information regarding how the Data Breach occurred.

12. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their private information and are subject to an increased risk of identity theft.

13. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practice appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' Private Information.

14. As a result of Defendant's inadequate digital security and notice process, Plaintiff's and Class Members' Private Information was exposed to criminals. Plaintiff and the Class Members have suffered and will continue to suffer injuries including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private

[6] *Id.*
[7] *Id.*

Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

15. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. Defendant's conduct amounts to at least negligence and violates federal and state statutes.

16. Plaintiff brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendant for: negligence; negligence per se; unjust enrichment, breach of contract, invasion of confidence.

17. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

## PARTIES

***Plaintiff***

18. Plaintiff E.H, a minor, is a resident of Ridgeway, Virginia. Plaintiff is a student at Henry County Public School District, which uses PowerSchool products. On January 9, 2025, Plaintiff's school sent an email notification informing families and staff about the Data Breach.[8] Upon information and belief, Plaintiff's Private Information was compromised in the Data Breach. As a result of the Data Breach, Plaintiff is now subject to substantial and imminent risk of future harm.

[8] *Exhibit 1*: E.H. Notice Email.

***Defendant***

19. Defendant PowerSchool Holdings, Inc. is a cloud-based software solution provider for K-12 schools and districts, and is headquartered in Folsom, California, having its principal place of business located at 150 Parkshore Drive, Folsom, California 95630.[9]

## JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount of controversy exceeds $5 million, exclusive of interest and costs. There are over 100 putative Class Members. Plaintiff is a resident of a different state than Defendant.

21. This Court has personal jurisdiction over PowerSchool because it is headquartered in this district and conducts substantial business in this district. It has also conducted systematic and continuous activities in California; and there is a substantial nexus between the conduct PowerSchool directs at California and the claims asserted herein.

22. Venue is proper in this Court because Defendant is headquartered in this district.

## FACTUAL ALLEGATIONS

### A. Background on Defendant

23. Defendant is a cloud-based software solutions provider for K-12 schools and districts that supports over 60 million students and over 18,000 customers worldwide, and is headquartered in Folsom, California.[10]

24. Upon information and belief, Defendant made promises and representations to individuals', including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.[11]

---

[9] *Contact us,* PowerSchool Holdings, Inc.: https://www.powerschool.com/company/contact/ (last visited January 10, 2025).

[10] *PowerSchool Holdings, Inc*.: https://www.powerschool.com/company/ (last visited January 10, 2025).

[11] *Privacy*, PowerSchool Holdings, Inc. https://www.powerschool.com/privacy/ (last visited January 10, 2025).

25. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

26. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Members' Private Information from disclosure to third parties.

**B. The Data Breach**

27. On December 28, 2024, Defendant became aware of a security incident on its IT Network.[12] Defendant launched an investigation to determine the nature and scope of the incident.[13]

28. The investigation determined that an unauthorized third-party gained access to Defendant's IT Network between December 22, 2024, and December 28, 2024. and obtained individuals' sensitive Private Information through Powerschool's customer support portal, PowerSource.[14]

29. The investigation determined that an unauthorized third-party gained access to PowerSource by using compromised credentials.[15]

30. Upon information and belief, Defendant's investigation determined that the following types of Private Information were compromised in the Data Breach: name, addresses, phone number, Social Security number, grade point average, bus stop, password, note, alert, student ID number, parent information, and medical information.[16]

31. Defendant failed to take precautions designed to keep individuals' Private Information secure.

---

[12] Lawrence Abrams, *PowerSchool hack exposes student, teacher data from K-12 districts* (January 7, 2025) https://www.bleepingcomputer.com/news/security/powerschool-hack-exposes-student-teacher-data-from-k-12-districts/ (last visited January 10, 2025).
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*

32. Plaintiff's claims arise from Defendant's failure to safeguard her Private Information and failure to provide timely notice of the Data Breach.

33. Defendant failed to take precautions designed to keep individuals' Private Information secure.

34. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

35. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

**C. Defendant's Failure to Prevent, Identify, and Timely Report the Data Breach**

36. Defendant admits that unauthorized third persons accessed its network systems. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

37. The Private Information that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

38. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[17] Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard individuals' sensitive Private Information.

39. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[18] Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

---

[17] *Protecting Personal Information: A Guide for Business,* FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited January 10, 2025).

[18] *Id.*

40. Here, Defendant failed to provide immediate notice after being made aware of the Data Breach to notify impacted individuals.

**D. The Harm Caused by the Data Breach Now and Going Forward**

41. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). When "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[19]

42. The type of data that may have been accessed and compromised here – such as names and Social Security numbers – can be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access. Social Security numbers and dates of birth together constitute high risk data.

43. Plaintiff and Class Members face a substantial risk of identity theft given that their Social Security numbers, addresses, dates of birth, and other important Private Information were compromised in the Data Breach. Once a Social Security number is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

44. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

45. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.[20]

---

[19] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited January 10, 2025).

[20] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited January 10, 2025).

46. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity."[21] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [PII] belonging to victims from countries all over the world."[22] As data breaches continue to reveal, "PII about employees, customers and the public are housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[23]

47. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[24] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[25]

48. A compromised or stolen Social Security number cannot be addressed as simply as a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[26]

---

[21] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited January 10, 2025).
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited January 10, 2025).
[26] *Id.*

49. The Private Information compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director of the cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[27]

50. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[28]

51. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[29] Defendant did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen. Defendant failed to provide immediate notice after learning of the Data Breach.

52. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their

---

[27] *Experts advise compliance not same as security*, RELIAS MEDIA (Mar. 1, 2015) https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (last visited January 10, 2025).

[28] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited January 10, 2025).

[29] *Id.*

personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

53. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

54. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff's and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

55. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

## CLASS ALLEGATIONS

56. Plaintiff brings this class action under Code of Civil Procedure § 382, individually and on behalf of all members of the following Class:

All United States citizens whose Private Information was compromised in the Data Breach (the "Class").

57. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

58. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

59. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

60. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, upon information and belief, Plaintiff estimates that the Class is comprised of hundreds of thousands of Class Members, if not more. The Class is sufficiently numerous to warrant certification.

61. Typicality of Claims: Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class, had her Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and her claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

62. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

63. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual

Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

64. Predominant Common Questions: The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendant's storage of Plaintiff's and Class Member's Private Information was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiff's and Class Members' Private Information;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiff's and Class Members' privacy;

g. Whether Defendant's conduct violated the statutes as set forth herein;

h. Whether Defendant took sufficient steps to secure individuals' Private Information;

i. Whether Defendant was unjustly enriched; and

j. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

65. Information concerning Defendant's policies is available from Defendant's records.

66. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

67. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct

for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

68. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

69. Given that Defendant had not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

## CAUSES OF ACTION

### COUNT I
### NEGLIGENCE
### (On Behalf of Plaintiff and the Class)

70. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 18 and paragraphs 24 through 60 as though fully set forth herein.

71. Plaintiff brings this claim individually and on behalf of the Class Members.

72. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

73. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

74. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within its possession was compromised and precisely the types of information that were compromised.

75. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its

systems and networks, and the personnel responsible for them, adequately protected individuals' Private Information.

76. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

77. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

78. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information.

79. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems; and

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

80. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

81. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

82. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

83. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff's and Class Members' Private Information. In violation of the FTC guidelines, *inter alia,* Defendant did not protect the personal patient information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

84. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

85. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

86. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

87. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

88. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

89. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs

associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

**COUNT II**
**NEGLIGENCE *PER SE***
**(On Behalf of Plaintiff and the Class)**

90. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 17 and paragraphs 23 through 55 as though fully set forth herein.

91. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

92. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and by failing to comply with industry standards.

93. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

94. Class Members are customers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

95. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

96. As a result of Defendant's negligence *per se*, Plaintiff and Class Members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

**COUNT III**
**UNJUST ENRICHMENT**
**(On behalf of Plaintiff and the Class)**

97. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 17 and paragraphs 23 through 55 as though fully set forth herein.

98. Plaintiff and Class Members conferred a benefit upon Defendant by using Defendant's consulting services and/or being employed by Defendant.

99. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff. Defendant also benefited from the receipt of Plaintiff's and Class Members' Private Information, as this was used for Defendant to administer its services to Plaintiff and the Class.

100. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Class Members' services and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendant or utilized its services had they known Defendant would not adequately protect their Private Information.

101. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach it caused.

**COUNT IV**
**BREACH OF CONTRACT**
**(On behalf of Plaintiff and the Class)**

102. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 17 and paragraphs 23 through 55 as though fully set forth herein.

103. Plaintiff and Class Members, upon information and belief, entered into express contracts with Powerschool that included Powerschool's promise to protect nonpublic Private Information given to Powerschool or that Powerschool gathered on its own, from disclosure.

104. Plaintiff and Class Members performed their obligations under the contracts when they provided their Private Information to Powerschool in exchange for consulting services and when they paid for the consulting service provided by Powerschool, or employment.

105. Powerschool breached its contractual obligations to protect the nonpublic Private Information which Powerschool possessed and was entrusted with when the information was accessed by unauthorized persons as part of the data breach.

106. As a direct and proximate result of Powerschool's above-described breach of contract, Plaintiff and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

**COUNT V**
**BREACH OF CONFIDENCE**
**(On Behalf of Plaintiff and the Class)**

107. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 17 and paragraphs 23 through 55 as though fully set forth herein.

108. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information that Plaintiff and Class Members entrusted to Defendant.

109. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

110. Plaintiff and the Class entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

111. Plaintiff and the Class also entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

112. Defendant voluntarily received Plaintiff's and Class Members' Private Information in confidence with the understanding that their Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

113. As a result of Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

114. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class have suffered damages.

115. But for Defendant's disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information as well as the resulting damages.

116. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendant knew or should have known its methods of accepting and securing Plaintiff's and Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' Private Information.

117. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of current and former people; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

118. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and her counsel as Class Counsel;

(b) For an order declaring that Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) For an award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

## JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

*[SIGNATURE BLOCKS ON FOLLOWING PAGE]*

Dated: January 13, 2025

Respectfully Submitted,

By: /s/ *John J. Nelson*

John J. Nelson (SBN 317598)
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Eduard Korsinsky*
Mark Svensson*
**LEVI & KORSINSKY, LLP**
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: ek@zlk.com
Email: msvensson@zlk.com

*Attorneys for Plaintiff and the Proposed Class*

**pro hac vice* forthcoming